[00175] WHAT IS CLAIMED IS:

We claim:

1. A system for maintaining security in a distributed computing environment, comprising:

(1) a business logic manager, coupled to a network, including

a database for storing a security policy including a plurality of rules; and

a policy distributor, coupled to the database, for distributing the rules through the network;

(2) a security engine, coupled to the network, for storing a set of rules received through the network from the policy distributor and for enforcing the rules; and

(3) an application, coupled to the security engine.

2. The system of claim 1, wherein the rules are separate from the application.

3. The system of claim 1, wherein the security engine further comprises:

an engine for, based on the rules, evaluating a request to access the application; and

an application programming interface (API) for enabling the application to communicate with the engine.

4. The system of claim 3, wherein the security engine further comprises:

a plug-in application programming interface (plug-in API) for extending capabilities of the security engine.

5. The system of claim 1, further comprising:

location means for enabling components in the system to locate each other through the network.

6. The system of claim 1, wherein the policy manager and the policy distributor are hosted on a first server, the security engine and the application are hosted on a second server, and the first and second servers are communicatively coupled to each other through the network.

7. A system for maintaining security for an application in a distributed computing environment, comprising:

an engine, coupled to a network, for storing a set of rules received through the network from a centralized location and for enforcing the rules;

an interface coupled to the engine; and

an application, coupled to the interface to enable the application to communicate with the engine.

8. The system of claim 7, wherein the rules are separate from the application.

9. The system of claim 7, further comprising:

a plug-in application programming interface (plug-in API) for extending capabilities of the security engine.

10. A system for maintaining security in a distributed computing environment, comprising

(1) a policy manager, coupled to a network, including

a database for storing a security policy including a plurality of rules;

a policy distributor for distributing the rules through the network;

(2) a plurality of security engines, each coupled to the network, for receiving a set of rules through the network from the policy distributor, storing the set of rules, and enforcing the set of rules; and

(3) a plurality of applications, each application being coupled to a respective security engine, each security engine being able to enforce a set of rules for its respective application.

11. The system of claim 10, wherein the rules are separate from each application.

12. The system of claim 10, wherein each security engine further comprises:

an engine for, based on a set of rules, evaluating a request to access a particular application; and

an application programming interface (API) for enabling a respective application to communicate with a respective engine.

13. The system of claim 12, wherein each security engine further comprises:

a plug-in application programming interface (plug-in API) for extending capabilities of the security engine.

14. The system of claim 10, further comprising:

location means for enabling components in the system to locate each other through the network.

15. The system of claim 10, wherein the policy manager and the policy distributor are hosted on a policy server, the plurality of security engines and the plurality of applications are hosted on at least one separate server, and the policy server is communicatively coupled through the network to the separate server.

16. A system for maintaining security for a plurality of applications in a distributed computing environment, comprising:

an engine, coupled to a network, for storing a set of rules received through the network from a centralized location, and for enforcing the rules;

a plurality of interfaces coupled to the engine; and

a plurality of applications, each application being coupled to a respective interface to enable the application to communicate with the engine through its respective interface, wherein the engines enforcing the rules for the application.

17. The system of claim 16, wherein the rules are separate from each application.

18. The system of claim 17, further comprising:

a plug-in application programming interface (plug-in API) for extending capabilities of the engine.

19. A system for distributing a security policy in a distributed computing environment, comprising:

(1) a policy manager, coupled to a network, including

a database for storing a first version of a policy including a plurality of rules;

updating means for entering a sequence of incremental changes to the rules in the first version of policy to generate a second version of a policy;

tracking means for tracking each of the incremental changes and for compiling a changed portion of the first version of the policy; and

a policy distributor for distributing the changed portion through the network;

(2) a security engine, coupled to the network, for storing the first version of the policy and for receiving the changed portion through the network, the security engine including means for using the changed portion to update the first version of the policy to create the second version of the policy, and for enforcing the second version of the policy for applications; and

(3) an application coupled to the security engine.

20. The system of claim 19, wherein each of the incremental changes of the current policy includes rule deletions, rule additions, or rule amendments.

21. The system of claim 19, further comprising:

location means for enabling components in the system to locate each other through the network.

22. A system for distributing a security policy in a distributed computing environment, comprising:

(1) a policy manager, coupled to a network, including:

a database for storing a first version of a policy including a plurality of rules;

means for entering a sequence of incremental changes to the rules in the first version of the policy to generate a second version of a policy;

means for tracking each of the incremental changes of the rules in the first version of the policy and for compiling a changed portion in the first version of the policy;

a policy distributor for distributing the changed portion through the network;

(2) a plurality of security engines, each security engine

being coupled to the network,

receiving the changed portion of the policy from the

policy distributor through the network,

storing a set of rules in the first version policy, and

including means for updating the first version of the policy to the second version of the policy based on the changed portion of the first version of the policy; and

(3) a plurality of applications, each application being coupled to its respective security engine which enforces the second version of the policy for the application.

23. The system of claim 22, wherein each of the incremental changes of the current policy includes rule deletions, rule additions, or rule amendments.

24. The system of claim 23, further comprising:

location means for enabling components in the system to locate each other through the network.

25. A system for distributing a security policy in a distributed computing environment, comprising:

(1) a policy manager, coupled to a network, including

a database for storing a first version of a policy including a plurality rules;

updating means for entering a sequence of incremental changes to the rules in the first version of the policy to generate a second version of a policy;

tracking means for recording a respective delta change for each of the incremental changes;

reversing means for generating a reversed portion of the second version of the policy based on the sequence of delta changes;

a policy distributor for distributing the reversed portion through the network;

(2) a security engine, coupled to the network, for storing the second version of the policy and for receiving the reversed portion through the network from the policy distributor, the security engine including means for restoring the second version of the policy to the first version of the policy based on the reversed portion, the security engine enforcing the restored first version of the policy for the applications; and

(3) an application coupled to the security engine.

26. The system of claim 25, wherein each of the incremental changes of the current policy includes rule deletions, rule additions, or rule amendments.

27. The system of claim 26, further comprising:

location means for allowing components in the system to locate each other through the network.

28. A system for analyzing a security policy in a distributed computing environment, comprising:

(1) a business logic manager, coupled to a network, including

a database for storing a security policy including a plurality of rules;

a policy analysis engine for analyzing a policy analysis query, the policy analysis engine further including

(i) an interpret module for interpreting the policy analysis query,

(ii) a search module for searching the policy stored in the database, in response to the interpreted policy analysis query, to provide an answer to the policy analysis query , and

(iii) a displaying module for displaying the answer; and

a policy distributor for distributing the rules through the network;

(2) a security engine, coupled to the network, for storing a set of rules received through the network from the policy distributor and for enforcing the set of the rules; and

(3) an application, coupled to the security engine.

29. The system of claim 28, wherein the policy analysis query contains a subject filed, a privilege field, or a resource filed, and the interpreter module interprets the policy query based on the resource field, the privilege field, or the resource field.

30. The system of claim 29, wherein the policy analysis query is a policy query, a verification query, or a cross-referencing query.

31. A system for analyzing a security policy in a distributed computing environment, comprising:

(1) a business logic manager, coupled to a network, including

a global database for storing a global security policy including a plurality of rules; and

a policy distributor, coupled to the database, for distributing the rules through the network;

(2) a business logic engine, coupled to the network, including

(i) a local policy database for storing a local security database including a set of the rules, received from the policy distributor through network, in the global security polity,

(ii) a policy analysis engine for analyzing a policy analysis query,

(iii) an interpret module for interpreting the policy analysis query,

(iv) a search module for searching the local security policy stored in the local policy database, in response to the interpreted policy analysis query, to provide an answer to the policy analysis query, and

(v) a displaying module for displaying the answer; and

(3) an application, coupled to the security engine.

32. The system of claim 31, wherein the policy analysis query contains a subject filed, a privilege field, or a resource filed, and the interpreter module interprets the policy query based on the resource field, the privilege field, or the resource field.

33. The system of claim 31, wherein the policy analysis query is a policy query, a verification query, or a cross-referencing query.